

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

RECEIVED

JAN 27 1999

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of)
)
Communications Assistance for)
Law Enforcement Act)
_____)

CC Docket No. 97-213

SPRINT PCS REPLY COMMENTS

Jonathan M. Chambers
Vice President, Sprint PCS
1801 K Street, N.W., Suite M112
Washington, D.C. 20006
(202) 835-3617

Joseph Assenzo
General Attorney, Sprint PCS
4900 Main, 12th Floor
Kansas City, MO 64112
(816) 559-2514

January 27, 1999

No. of Copies rec'd 0+4
List ABCDE

Table of Contents

Summary of Reply Comments	iii
I. Costs Are Relevant	2
II. CALEA Does Not Authorize the Commission to Order Carriers to Provide Entirely New Capabilities Never Before Made Available	7
III. The FBI Has Failed to Demonstrate That The Punch List Capabilities Are Reasonably Available to Carriers	13
IV. The FBI's Refusal to Share Cost Data That It Uniquely Possesses Is Itself Grounds to Reject Its Deficiency Petition	15
VII. Conclusion.....	21

Summary of Reply Comments

Sprint PCS demonstrates that there are three independent reasons why the Commission must deny the FBI's Section 107(b) "deficiency" petition: (1) CALEA does not authorize the Commission to order the industry to provide entirely new interception capabilities such as those contained in the FBI's "punch list;" (2) the FBI has still failed to demonstrate that its punch list items involve capabilities that are reasonably available to carriers; and (3) the FBI has failed to demonstrate that its proposed capabilities can be implemented by cost-effective methods that will have minimal impact on the rates paid by residential consumers.

**Before the
Federal Communications Commission
Washington, D.C. 20554**

RECEIVED

JAN 27 1999

**FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY**

In the Matter of)	
)	
Communications Assistance for)	CC Docket No. 97-213
Law Enforcement Act)	
_____)	

SPRINT PCS REPLY COMMENTS

Sprint Spectrum L.P., d/b/a Sprint PCS ("Sprint PCS"), submits this reply to the comments filed by the Department of Justice and the Federal Bureau of Investigation (collectively, "FBI" or "FBI Comments"). Sprint PCS demonstrates below that there are three independent reasons why the Commission must deny the FBI's Section 107(b) "deficiency" petition: (1) CALEA does not authorize the Commission to order the industry to provide entirely new interception capabilities such as those contained in the FBI's "punch list;" (2) the FBI has still failed to demonstrate that its punch list items involve capabilities that are reasonably available to carriers; and (3) the FBI has failed to demonstrate that its proposed capabilities can be implemented by cost-effective methods that will have minimal impact on the rates paid by residential consumers.¹

¹ Consistent with FCC precedent, the burden is on the petitioner, here the FBI, to demonstrate its entitlement to the relief it seeks. *See, e.g.,* U S WEST at 2-7; Bell Atlantic Mobile at 5-9.

I. Costs Are Relevant

The FBI would have the Commission believe that law enforcement's very ability to do its job will be crippled unless the industry implements both the J-Standard and its "punch list" items:

The outcome of this process will determine whether . . . law enforcement's ability to investigate, prosecute, and prevent crimes will be compromised.²

This assertion is not supported by the facts.

At the outset, the Commission needs to remember that electronic surveillance represents only a small portion of law enforcement's efforts.³ The most prevalent way that carriers assist law enforcement is through the production of call detail records in response to subpoenas. During the last few months of 1998, for instance, Sprint PCS produced an average of 500 call detail records each month — a figure that undoubtedly will increase as Sprint PCS launches additional markets (*e.g.*, Atlanta, Chicago, Cleveland, Las Vegas).

The Commission must also understand that implementation of neither the J-Standard nor the FBI punch list is necessary for law enforcement to conduct effective interceptions — even on advanced CMDA networks like that operated by Sprint PCS. Last year, for example, Sprint PCS conducted a total of 554 interceptions (Title III call con-

² FBI Comments at 6.

³ For example, during 1997 state and federal judges approved a total of 1,186 Title III wiretaps — or about three per day. *See* Report of the Director of the Administrative office of the U.S. Courts, *Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications* (April 1988).

tent, pen register, trap and trace) on behalf of state and federal law enforcement.⁴ It is noteworthy that the New York Police Department readily acknowledges that CMRS carriers “*already provide law enforcement a significant portion of the capabilities described in the industry’s J-STD-025.*”⁵ Indeed, Sprint PCS, *at its own expense and initiative*, has modified its network so law enforcement today can receive a robust set of capabilities, including:

- Three-way calling;
- Numbers of the calling and called parties;
- Any call forwarding number;
- Cell site/sector information;
- Notification of over the air activation features; and
- Call start and end time.

Moreover, Sprint PCS has engineered its network so law enforcement can receive this and other call-identifying information at their own premises on a near real time basis (*e.g.*, within four to six seconds of the events occurring).⁶

While its analysis is not complete, Sprint believes that its existing law enforcement interception support system very likely complies with the capability requirements

⁴ With a customer base approximating two million during this period, law enforcement conducted some type of interception on less than one-quarter of one percent (0.0277%) of Sprint PCS’s customers.

⁵ NYPD Comments at 2 (emphasis added).

⁶ Sprint PCS has been charging law enforcement only \$25 daily for each interception — a fee well below its actual cost. Needless to say, any government mandate imposing huge new costs on Sprint PCS would compel it to increase dramatically the fee it charges law enforcement to conduct interceptions.

set forth in Section 103 of CALEA. As the FBI itself has acknowledged, carriers are not required to implement the industry standard as a condition to satisfying CALEA's requirements.⁷ While implementation of the J-Standard *might* provide certain additional benefits (*e.g.*, access to call-identifying information in real time as opposed to five seconds after the events; new signaling messages such as the "CCOpen Message Parameters – DDU TYPE"), Sprint PCS has recently learned that the cost to implement the J-Standard would be staggering — and would not begin to outweigh any relatively minor incremental benefits that the J-Standard might provide.⁸

Sprint PCS's major manufacturers have advised Sprint PCS that it would have to spend, at a minimum, \$41.7 million to acquire and install J-standard software in its network as it existed at the end of 1998. Based on network expansions planned during 1999, this sum would increase to over \$50 million — and to over \$60 million if network expansions during year 2000 are included.

It is important to emphasize that these are conservative figures. Sprint PCS's manufacturers have indicated that it can expect to pay additional sums for unspecified hardware necessary to provide certain capabilities. In addition, one of Sprint PCS's ven-

⁷ See, *e.g.*, FBI Deficiency Petition at 3-4 ¶ 2 (March 27, 1998)("[C]ompliance with the industry standard is merely one way of assuring compliance with Section 103; a carrier can satisfy its obligation by any means that meet Section 103's underlying assistance capability requirements."). See also H.R. No. 103-827, at 23 (Oct. 4, 1994)("The legislation leaves it to each carrier to decide how to comply."); *id.* at 27 ("Compliance with the industry standards is voluntary, not compulsory. Carriers can adopt other solutions for complying with the capability requirements.")(hereinafter, "House Report").

⁸ The FBI misstates the record when it states that industry agreed "to incur these costs by adopting the J-Standard, and they will be incurred whether or not the Commission modifies the J-Standard to add capabilities from the government's punch list." FBI Comments at 17. The J-Standard represents a technical specification prepared by technical subject matter experts. However, there certainly was no agreement that industry would implement the J-Standard — espe-

dors has stated that *yet additional sums may be required simply to maintain the current quality of its network*:

The List Prices do not include modifications that may be required to existing carrier equipment to retain the same level of network performance, capabilities and capacity.⁹

These sums would be expended so that law enforcement might receive certain information in a different format or time frame than they receive today with Sprint PCS's current interception support system.

The FBI's response to these enormous costs is unhelpful: "those costs are irrelevant."¹⁰ To Congress, the Commission, Sprint PCS and its customers, however, these costs are quite relevant. Indeed, two of the four statutory factors the Commission must apply in this proceeding specifically address the cost impact of requested features.¹¹ Moreover, Congress understood fully that the FBI, to the extent it was not constrained by a budget, would have an incentive to "gold plate" its demands. It was for this very reason that Congress expressly charged the Commission to address this "gold plating" incentive:

The costs of assuring that new switches and services be accessible for wiretapping are unknown at this time. They may be de minimis or they may be substantial. Our compromise provides that the Federal Communications will resolve questions associated with who between the industry and the government shall bear these costs. The Commission . . . would determine . . . (1) Whether the costs of meeting the wiretap capability requirements of law enforcement shall be borne by the government or should be assumed by the telecommunications carriers . . . (3) What meth-

cially since the costs of implementing the Standard were not known at the time it was developed. Thus, the FBI (and the FCC) should expect numerous carriers to file Section 109 petitions.

⁹ This sentence is a quotation from a response submitted by one of Sprint PCS's vendor. The vendor has asked Sprint not to reveal its identity or the details of its costs estimates, and it is for this reason that Sprint PCS does not attach this document.

¹⁰ FBI Comments at 17.

¹¹ See 47 U.S.C. § 100(b)(1) and (3).

ods best ensure that there will be no “goldplating” . . . by the government asking for upgrades that are unnecessary . . . ; (4) How to ensure that whatever method is selected is competitively neutral, has a minimum effect on the deployment of an advanced telecommunications network and minimum adverse effect on telephone rates.¹²

Congress imposed on the Commission the task of ensuring that law enforcement is not “gold plating” its requests. In addition to the J-Standard, law enforcement wants the industry to implement the FBI punch list items. Although the punch list involves capabilities never before provided to law enforcement, the FBI claims that the absence of these new features “not only will lead to the loss of evidence . . . but also may limit the evidentiary value of the evidence that law enforcement does acquire.”¹³ Given that law enforcement never received these punch list features in the past, Sprint PCS cannot concur in the FBI’s assertions.

Sprint PCS, in response to the Commission’s request for cost data, asked its manufacturers for cost estimates of the FBI punch list capabilities. Only one of its vendors was willing to share any data, and this one vendor’s estimates were very preliminary. This vendor stated that, including known new hardware costs, implementation of the punch list could approximate 50% of the cost of the J-standard itself. (This estimate did not include any modifications to Sprint PCS’s new data network.) As documented above, Sprint PCS has been willing to expend capital and devote resources to meet the legitimate needs of law enforcement. However, on behalf of its customers (who will invariably pay for the increase in interception costs), Sprint PCS has an obligation to oppose the unreasonable and unrealistic demands of the FBI.

¹² See House Report at 49.

¹³ FBI Comments at 63.

II. CALEA Does Not Authorize the Commission to Order Carriers to Provide Entirely New Capabilities Never Before Made Available

The FBI has asked the Commission to order carriers to provide new interception capabilities so law enforcement can obtain new information and expand the type of electronic surveillance that it may conduct. The FBI notes that advanced technologies can often be designed to provide “information that ha[s] not traditionally been available over the local loop,” and it asserts that accessing these new capabilities “could” be “important” in law enforcement’s surveillance efforts.¹⁴

Sprint PCS obviously is not in a position to determine what capabilities may, or may not, be important to law enforcement surveillance. However, it is clear that CALEA does not empower the Commission to grant the FBI’s requested relief because CALEA was designed to preserve the *status quo* — not expand the information made available to law enforcement.

As the FBI recommends, the Commission should consider the FBI’s “punch list” capabilities “in the broad context of CALEA’s underlying statutory objective.”¹⁵ Congress enacted CALEA because “the FBI had identified specific instances in which law enforcement agencies were precluded due to technological impediments from fully implementing authorized electronic surveillance.”¹⁶ According to the FBI, the problem was that law enforcement’s ability to conduct lawful interceptions was being thwarted as a result of the proliferation of “advanced technologies such as digital or

¹⁴ See FBI Comments at 27 and 38.

¹⁵ *Id.* at 6.

¹⁶ House Report at 14.

wireless transmission.”¹⁷ The FBI claimed before Congress that these advanced technologies often precluded law enforcement from conducting surveillance as it had in the past (*i.e.*, tapping an analog local loop).¹⁸ *But see* NYPD Comments at 2 (“[W]ireless [carriers] already provide law enforcement a significant portion of the capabilities described in the industry’s J-STD-025.”)

CALEA addressed this concern by specifying that, as a general rule, the deployment of advanced technologies should not cripple law enforcement’s ability to continue to conduct lawful interceptions.¹⁹ However, in addressing this concern, Congress did not authorize law enforcement to obtain new surveillance powers or to expand the type of capabilities carriers would be required to offer law enforcement. To the contrary, Congress was very clear that CALEA’s purpose was “to *preserve* the government’s ability . . . to intercept communications involving advanced technologies”:

The legislation requires telecommunications common carriers to ensure that new technologies and services *do not hinder* law enforcement access to the communications of a subscriber The bill *will preserve* the government’s ability . . . to intercept communications The Committee expects industry, law enforcement and the FCC to *narrowly interpret* the requirements.²⁰

¹⁷ *Id.* at 16.

¹⁸ *See* FBI Comments at 25.

¹⁹ Congress did make clear that one of CALEA’s core policies is “to avoid impeding the development of new communications services and technologies” and that if “a service or technology *cannot* reasonably be brought into compliance with the interception requirements, then the service or technology *can* be deployed.” House Report at 13 and 19 (emphasis in original).

²⁰ House Report at 9, 16, and 22 (emphasis added). *See also id.* at 49 (“It is essential that we provide a means of assuring that law enforcement agencies are *not impaired* by new telephone switching technology as they carry out lawful wiretaps.”)(emphasis added).

The House of Representatives further confirmed CALEA's limited focus as they voted on the legislation. The statements of Representative Oxley are illustrative of the prevalent view in Congress:

*I want to emphasize that this measure would not expand the authority of law enforcement in any way. [The bill] would merely ensure that it remains technically feasible to access communications. Those who suggest that this legislation gives Government new power to pry into people's lives are simply mistaken.*²¹

See also Statement of Mr. Markey ("The Federal Bureau of Investigation argues that as these advanced technologies get deployed, that the technology should not, in essence, repeal or modify the 1968 Wiretap Act. Instead, the Bureau argues, we must update and clarify our laws so that their ability to conduct wiretaps is *maintained* — *not expanded or diminished* — *just maintained*.").²²

That CALEA was limited to preserving preexisting interception capabilities with digital technologies — as opposed to providing for entirely new capabilities — is a point that even the FBI Director readily acknowledged at the time:

The FBI Director testified that the legislation was intended to *preserve the status quo*, that it was intended to provide law enforcement *no more and no less access to information than it had in the past*.²³

²¹ 140 Cong. Record H10782 (Oct. 4, 1994)(emphasis added). *See also* Statement of Rep. Brooks, 140 Cong. Record H10779 (Oct. 4, 1994)("Finally, it is also worth noting that this bill does not expand law enforcement authority to conduct these interceptions. In fact, the bill includes several provisions to improve the privacy and security in the telecommunications network.").

²² 140 Cong. Record H10780 (Oct. 4, 1994)(emphasis added).

²³ House Report at 22 (emphasis added). *See also* October 4, 1994 letter from FBI Director to the House of Representatives, 140 Cong. Record H10782 (Oct. 4, 1994)("If enacted, this legislation will prevent new telecommunications technologies from continuing to impede law enforcement agencies' lawful conduct of court-ordered electronic surveillance.").

The FBI has, moreover, confirmed this position in its comments, noting that “information that traditionally has been available to law enforcement in the POTS environment does provide, in our view, a useful reference point in resolving disputes over reasonable availability”:

As explained in our earlier filings, Congress’s underlying purpose in enacting CALEA was “to ensure that new technologies and services do not hinder [authorized] law enforcement access” to wire and electronic communications. . . . [T]he fact that such information has traditionally been available to law enforcement . . . should be given considerable weight . . .

²⁴

In evaluating the FBI’s petition, then, the Commission must first determine whether the FBI is seeking to (a) preserve a preexisting capability (one that has been available with analog technologies), or (b) obtain new information from new capabilities. CALEA authorizes the former, but not the latter. As the FBI Director himself testified, CALEA provides law enforcement with “no more and no less access to information than it had in the past.”²⁵

The FBI concedes that in its punch list it seeks new information and capabilities that were not provided in the past. For example, the industry agrees that law enforcement should be able to intercept conference calls supported by digital networks, a capability law enforcement enjoyed in the past with analog technologies.²⁶ The FBI, however, is now dissatisfied with the *status quo*; and it wants an entirely new capability

²⁴ FBI Comments at 27. However, as the FBI correctly notes and as discussed more fully below, “[i]nformation that has traditionally been available on the local loop may not invariably be reasonably available to the carrier when surveillance is implemented at the switch.” *Id.* at 26.

²⁵ House Report at 22.

²⁶ See J-STD-025 § 4.5.1 (“The Circuit IAP (CIAP) shall access a multi-party circuit-mode communication (e.g., Three-Way Calling, Conference Calling, or Meet Me Conferences) as it would be presented to the intercept subject.”).

so it can intercept a conference call even when the subject of the court order leaves the call or places the call on hold.²⁷

The FBI's requested "conference hold" feature raises serious issues under the Fourth Amendment as well as our privacy laws, because law enforcement wants to intercept communications when the subject of the court order is not even participating in the call.²⁸ As U S WEST observes, "[f]or the first time, a person's private conversations would be subject to interception simply because he *previously* was on a conference call with an intercept subject."²⁹ However, the Commission need not address these constitutional issues because the FBI concedes that its "conference hold" feature is a new capability.³⁰ As Senator Leahy has also observed:

Certain of these punch list items appear far beyond the scope and intent of CALEA, such as . . . the FBI's wish for the capability to eavesdrop on conference call parties, who have been put on hold by the subject of the wiretap.³¹

Consequently, CALEA does not authorize the Commission to order carriers to provide the requested "conference hold" capability.

As the FBI notes, advanced technologies can often be designed to provide new interception capabilities such as the "conference hold" feature,³² and it is perhaps

²⁷ The FBI readily acknowledges that the "conference hold" feature it seeks is a new capability never before made available to law enforcement. *See* FBI Deficiency Petition at ¶ 51 (March 27, 1998).

²⁸ *See, e.g.*, EPIC/EFF/ACLU at 24.

²⁹ U S WEST at 13 (emphasis in original).

³⁰ *See* FBI Deficiency Petition at ¶ 51 (March 27, 1998)(Proposed "conference hold" feature would "not amount to a reduction in the information that has been available to law enforcement under POTS.").

³¹ Letter from Senator Patrick Leahy to Hon. Janet Reno and Louis J. Freeh, at 2 (Feb. 4, 1996).

³² *See* FBI Comments at 27.

understandable that law enforcement would want to take advantage of this new potential (especially if it can get others to pay for the capability).³³ But the fact remains that CALEA does not give this Commission the authority to order carriers to provide new capabilities to law enforcement, much less provide new capabilities at no charge to the government. As Representative Markey stated, CALEA is designed to ensure that law enforcement's ability to conduct interceptions is "maintained — not expanded or diminished — just maintained."³⁴

Thus, if the FBI wants access to new capabilities made possible by certain advanced technologies, it must return to Congress to receive the necessary authorization.³⁵

III. The FBI Has Failed to Demonstrate That The Punch List Capabilities Are Reasonably Available to Carriers

The surveillance capabilities that carriers must provide to law enforcement are set forth in Section 103 of CALEA, and Section 103(a)(2) contains an important limitation on the type of assistance that carriers must support: they must provide only that call-identifying information that "is reasonably available to the carrier."³⁶ Congress made very clear that "if such information is not reasonably available," then "a carrier

³³ See, e.g., International Association of Chiefs of Police at 1 ("As technology continues to grow, it is imperative to public safety that law enforcement's abilities grow at a comparable rate.").

³⁴ See footnote 21 and accompanying text.

³⁵ As the FCC has observed, an alternative is for the FBI ask the industry to develop features or capabilities beyond those required by CALEA. See *NPRM* at ¶ 35. Of course, as with any other customer, the FBI will be expected to pay for the development and deployment costs of any new capabilities it seeks.

³⁶ 47 U.S.C. § 1002(a)(2).

does not have to modify its system to make it available.”³⁷ As even the FBI acknowledges, “we would not go so far as to suggest that all information that had traditionally been available to law enforcement pursuant to its pen register authority is *ipso facto* ‘reasonably available’” in a digital, switch-based interception model.³⁸

Section 107(b) sets forth the standards that the FBI must meet to prevail in its deficiency petition, and one of these criteria is that the FBI demonstrate that the capability it seeks “meet[s] the assistance capability requirements of section 103 of this title by cost-effective methods.”³⁹ With respect to call-identifying information, the FBI’s burden of proof therefore has three components: (1) the information it seeks is call-identifying information within the scope of CALEA; (2) the information is “reasonably available” to the carrier; and (3) the information can be provided “by cost-effective methods.”

The industry comments filed in this proceeding establish that most of the information the FBI seeks is not call-identifying information as that term is defined in CALEA. However, the FBI’s petition suffers from two additional flaws: the FBI makes no attempt to demonstrate that any of the information it seeks is *either* “reasonably available” to carriers *or* can be provided by “cost-effective methods.”

The FBI attempts to divert attention from its fatal evidentiary omissions by encouraging the Commission to adopt a definition of “reasonably available” — a definition different than that adopted by the industry. The problem with the FBI’s particular

³⁷ House Report at 22.

³⁸ FBI Comments at 26.

³⁹ 47 U.S.C. 1006(b)(1).

proposal is that it does *not* define the statutory phrase “reasonably available,” but rather defines only the word “availability.” The FBI’s proposed definition provides:

Call-identifying information is reasonably available if (1) it is present in an element in the carrier’s network that is used to provide the subscriber with the ability to originate, terminate, or direct communications and (2) it can be accessed there, or can be delivered to an IAP located elsewhere, without unreasonably affecting the call processing capabilities of the network.⁴⁰

Under this FBI proposal, a carrier apparently must make any and all call-identifying information available to law enforcement so long as the information is “present” somewhere in the network and “can be delivered” to law enforcement — regardless of the difficulty or costs incurred in attempting to deliver this information to law enforcement.

As noted, Congress was very clear in specifying that only call-identifying information that “is reasonably available to a carrier” must be provided.”⁴¹ In determining what is, or is not, reasonably available, the Commission must necessarily evaluate the costs carriers would incur to provide requested information. The FBI’s suggestion that consideration of costs is irrelevant to the application of the reasonably available standard lacks merit and is inconsistent with the statutory “reasonably available” standard.

IV. The FBI’s Refusal to Share Cost Data That It Uniquely Possesses Is Itself Grounds to Reject Its Deficiency Petition

The cost of implementing the J-Standard/punch list will be enormous. The Attorney General recently advised Congress that the government alone would require “[i]n excess of \$2 billion” if Congress moved the current grandfather date of January 1,

⁴⁰ *Id.* at 25.

⁴¹ 47 U.S.C. § 1002(a)(2)(emphasis added).

1995.⁴² Industry estimates that the total implementation cost will be “between \$5 and 10 billion.”⁴³ Even the FBI’s estimated government implementation cost — \$0.5 billion originally budgeted, plus another \$2+ billion — would result in a new, additional cost of \$100,000 for each federal interception (assuming CALEA’s costs are amortized over five years and that the level of interceptions remains stable).⁴⁴ If the ultimate cost is closer to the industry estimates, the costs would be between \$200,000 and \$400,000 per federal interception order. This sum is *in addition to* the \$61,000 law enforcement already spends on average to implement a Title III interception.⁴⁵

The FBI acknowledges that implementation costs are a relevant statutory consideration in evaluating its “punch list” request.⁴⁶ In this regard, the FBI encourages “carriers . . . [to] provide the Commission with their own estimates of the costs associated with implementing CALEA’s assistance capability requirements” — even though it knows that carriers generally do not have access to this data at the present time.⁴⁷ Yet, although it has had “extensive consultations with manufacturers” and has obtained relevant cost data from most major vendors, the FBI refuses to disclose this cost data to the Commission and to carriers — even though *only* the FBI knows the total cost of CALEA

⁴² Letter from the Hon. Janet Reno, Luis J. Freeh, and Thomas A. Constantine to the Hon. Ted Stevens (Oct. 6, 1998).

⁴³ Letter from Thomas E. Wheeler, CTIA, to William Kennard, FCC Chairman, at 1 (Dec. 14, 1998).

⁴⁴ See EPIC/EFF/ACLU at n.9 (in 1996 federal agencies conducted a total of 5,150 interceptions: 3,262 pen registers; 1,307 trap and trace; and 581 wiretaps).

⁴⁵ See Report of the Director of the Administrative Office of the U.S. Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, at 10 (April 1998) (“[T]he average cost of an intercept order in 1997 was \$61,176.”).

⁴⁶ See FBI Comments at 11.

⁴⁷ See *id.* at 16.

implementation.⁴⁸ As explained below, the FBI's refusal to submit cost data is highly relevant to the statutory standard is itself grounds for the Commission to reject its punch list petition.

Sprint PCS would like to respond to the Commission's request for cost data. However, only one of its manufacturers was willing to share even preliminary estimates with it. As noted above, this vendor has told Sprint PCS that, including known new hardware costs, implementation of the punch list could approximate 50% (or more) of the cost of the J-Standard itself — a cost that does not include Sprint PCS's new data network.

The FBI is in an entirely different position. Earlier this year it obtained cost data from major manufacturers.⁴⁹ It is Sprint PCS's understanding that many vendors provided the FBI separate cost estimates for each capability on the FBI's punch list. Indeed, the FBI has advised Congress that “[s]ome solution providers were very receptive to the FBI's data requests, sharing detailed, per-capability and price data with law enforcement.”⁵⁰ Thus, not only does the FBI know what each vendor will likely charge for each punch list item, it also knows what the CALEA implementation costs will total nationwide. It bears emphasis that *only the FBI has access to this aggregate, nationwide cost data.*

Because of the FBI's unique access to relevant cost data, the industry specifically asked the FBI to submit with its FCC comments “cost information regarding the

⁴⁸ See *ibid.*

⁴⁹ See, e.g., DoJ/FBI, *CALEA Implementation Report to Congress*, at 5 (Jan. 26, 1998)(FBI notes its efforts to work with “solution providers” to develop “a CALEA solution price.”).

⁵⁰ *Id.* at 8 (emphasis added).

development and implementation of J-STD-025 and each of the Department of Justice's 'punch list' items."⁵¹ The FBI, however, has ignored this request, stating:

[W]e regretfully cannot disclose to the Commission any price information obtained from manufacturers.⁵²

None of the three reasons the FBI recites justify its refusal to provide cost data in its possession. The FBI first claims that it does not have cost data because manufacturers gave it "proposed prices, as distinct from underlying manufacturer costs."⁵³ However, manufacturer's prices are carrier's costs, and it is these vendor prices/carrier costs that will be passed on to consumers. Thus, manufacturer prices are the relevant data that the Commission should be evaluating in this proceeding.

Next, the FBI asserts it is prohibited from providing cost data because the information was submitted pursuant to non-disclosure agreements.⁵⁴ Industry is not asking the FBI to divulge the prices/costs of individual vendors. What is relevant to this proceeding is *aggregate* data, and only the FBI possesses such data. And importantly, submission of aggregate data is *not* covered by the non-disclosure agreements.⁵⁵

The FBI's final reason for not sharing available cost data with the Commission and industry is its contention that such data has marginal relevance to this proceeding. According to the FBI, "Congress has made a global determination that the bene-

⁵¹ CTIA/PCIA/TIA/USTA Letter to the Hon. Janet Reno (Dec. 4, 1998).

⁵² FBI Comments at 16.

⁵³ *Id* (emphasis in original).

⁵⁴ *Ibid*.

⁵⁵ See CTIA/PCIA/TIA/USTA Letter to the Hon. Janet Reno, at 1 (Dec. 4, 1998) ("We understand that individual submissions were subject to confidentiality agreements, but we are not aware that aggregate information is similarly protected.").

fits of requiring carriers to meet Section 103's assistance capability requirements exceeds the costs."⁵⁶ As a result, the FBI continues, the Commission's inquiry under Section 107(b) is limited to determining whether the punch list capability at issue "meet[s] the capability requirements of section 103":

The object of proceedings under Section 107(b) is not to decide whether carriers must comply with the assistance capability requirements of Section 103, but how they are to comply.⁵⁷

According to the FBI, "cost is relevant only as a basis for choosing among alternative means of meeting CALEA's assistance capability requirements — not as a basis for excusing compliance with those requirements."⁵⁸

The FBI's proposed interpretation of Section 107(b) is at complete odds with both the language of the statute and Congressional intent. The FBI would thus have the Commission re-write Section 107(b) to read:

If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that —

- (1) meet the assistance capability requirements of section 1002 of this title ~~by cost effective methods;~~
- (2) ~~protect the privacy and security of communications not authorized to be intercepted;~~
- (3) ~~minimize the cost of such compliance on residential ratepayers; [and]~~
- (4) ~~serve the policy of the United States to encourage the provision of new technologies and services to the public.~~

⁵⁶ FBI Comments at 12. Notably absent in the FBI Comments is any citation to this sweeping statement.

⁵⁷ FBI Comments at 11 (emphasis in original). *See also id.* at 1, 7, and 42.

⁵⁸ *Id.* at 2.

Congress did not, as the FBI asserts, adopt CALEA with a single “goal” — namely, to “insure that law enforcement can continue to conduct authorized wire-taps.”⁵⁹ Nor did Congress make “a global determination” that the “benefits of requiring carriers to meet” the FBI’s punch list “exceed the costs.”⁶⁰ To the contrary, Congress made abundantly clear that CALEA “seeks to balance three key policies”:

(1) to preserve *a narrowly focused* capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.⁶¹

In fact, Congress expressly declared that “[i]f a service or technology *can-not* reasonably be brought into compliance with the interception requirements, then the service or technology *can* be deployed.”⁶² In addition, CALEA’s authors expressly envisioned that the Commission “will resolve questions associated with who between the industry and the government shall bear these costs” and ensure both that there “will be no ‘goldplating’ . . . by the government for upgrades that are unnecessary” and that CALEA imposes a “minimum adverse effect on telephone rates.”⁶³

The Commission needs access to cost data to ensure that the FBI is not engaging in impermissible “gold plating.” As noted above, only the FBI has access to this cost relevant information. In light of the FBI’s refusal to share this critical data, Sprint PCS submits that the Commission has no choice but to assume that the data would estab-

⁵⁹ FBI Comments at 6.

⁶⁰ *Compare id.* at 12.

⁶¹ House Report at 13 (emphasis added).

⁶² *Id.* at 19 (emphasis in original).

⁶³ House Report at 49, Additional views of Representatives Edwards and Boucher.

lish that the punch list capabilities cannot be implemented by cost-effective methods and would negatively impact the rates paid by residential consumers.

V. Conclusion

Sprint PCS is committed to continuing to assist law enforcement in timely and efficiently meeting its legitimate interception needs. As noted in Part I above, Sprint PCS has modified its network so that law enforcement can today receive a robust set of interception capabilities — including CMRS location — on a real time and virtual real time basis.

Sprint PCS's position is driven by three considerations. First, Sprint PCS is compelled to protect the privacy interests of its customers because, as a practical matter, they do not have the opportunity to participate directly in this proceeding. In this regard, it is important that the Commission confirm Congress' own understanding of CALEA's requirements— that is, in the words of the FBI Director, CALEA provides law enforcement with “no more and no less access to information than it had in the past.”⁶⁴

Second, Sprint PCS seeks to protect the financial interests of its customers, because it will likely be they who will foot the bill for law enforcement's demands. Consistent with the plain language of the statute, it is critically important that CALEA be implemented by cost-effective means to minimize the impacts on competition and consumer rates.

Finally, as a new entrant that recently paid the federal government approximately \$3 billion to obtain its radio licenses, Sprint PCS is very troubled by the cur-

⁶⁴ See footnote 23 and accompanying text.


rent arbitrary grandfather/government reimbursement date of January 1, 1995. Absent modification, the current arrangement would give incumbent carriers, which already possess numerous incumbent advantages, an additional — and completely artificial — cost advantage in the marketplace.⁶⁵

Sprint PCS is not suggesting that the Commission has the authority to change this date. However, the Commission with its experience and knowledge does understand the competitive inequalities of the current arrangement. Sprint PCS therefore encourages the Commission to explain to Congress how this disparity can negatively impact the competitive balance within the industry.

Respectfully submitted

SPRINT SPECTRUM, L.P.,
d/b/a SPRINT PCS

By:


Jonathan M. Chambers
Vice President, Sprint PCS
1801 K Street, N.W., Suite M112
Washington, D.C. 20006
(202) 835-3617

Joseph Assenzo
General Attorney, Sprint PCS
4900 Main, 12th Floor
Kansas City, MO 64112
(816) 559-2514

January 27, 1999

⁶⁵ This competitive parity issue is by no means limited to the CMRS industry. For example, competitive LECs face a similar situation *vis-à-vis* incumbent LECs.

Certificate of Service

I, Tony Traini, hereby certify that on January 27, 1999, I caused to be served, by first-class mail, postage prepaid (or by hand where noted) copies of these reply comments.

*The Honorable William E. Kennard
Chairman
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*Ari Fitzgerald
Legal Advisor to Chairman Kennard
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*The Honorable Harold Furchtgott-Roth
Commissioner
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*Paul E. Misener, Senior Legal Advisor
to Commissioner Furchtgott-Roth
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*The Honorable Susan Ness
Commissioner
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*James Casserly
Legal Advisor to Commissioner Ness
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*The Honorable Michael Powell
Commissioner
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*Peter A. Tenhula
Legal Advisor to Commissioner Powell
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*The Honorable Gloria Tristani
Commissioner
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*Karen Gulick
Legal Advisor to Commissioner Tristani
Federal Communications Commission
The Portals
445 Twelfth Street, S.W.
Washington, D.C. 20554

*Christopher J. Wright
General Counsel
Federal Communications Commission
The Portals, Room 8C755
445 12th Street, S.W.
Washington, D.C. 20554

*Thomas Sugrue
Chief
Wireless Telecommunications Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

*Lawrence E. Strickling
Chief
Common Carrier Bureau
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

*Charlene Lagerwerff
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 8633
Washington, D.C. 20554

*Tejal Mehta
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W. Room 7115
Washington, D.C. 20554

*Tim Maguire
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 8038
Washington, D.C. 20554

*ITS
1231 20th Street, N.W.
Washington, D.C. 20036

*David Wye
Technical Advisor
Federal Communications Commission
2025 M Street, N.W., Room 5002
Washington, D.C. 20554

*Anna Gomez
Chief
Network Services Division
Common Carrier Bureau
Federal Communications Commission
2000 M Street, N.W., Room 235B
Washington, D.C. 20554

*Kent Nilsson
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W.
Washington, D.C.

*James Green
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., Room 7021
Washington, D.C. 20554

*Dale Hatfield
Office of Engineering and Technology
Federal Communications Commission
2000 M Street, N.W., Room 230
Washington, D.C. 20554

*Kimberly Parker
Wireless Telecommunications Bureau
Federal Communications Commission
2100 M Street, N.W., 7th Floor
Washington, D.C. 20554

Larry R. Parkinson
General Counsel
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

David. L. Sobel
Marc Rotenberg
Electronic Privacy Information Center
666 Pennsylvania Avenue, S.E.
Suite 301
Washington, D.C. 20003

Steven Shapiro
Cassidy Sehgal-Kolbet
American Civil Liberties Union
125 Broad Street
New York, New York 10004

Jerry Berman
James X. Dempsey
Center for Democracy and Technology
1634 Eye Street, N.W., Suite 1100
Washington, D.C. 20006

Matthew J. Flanigan
Grant Seiffert
Telecommunications Industry Association
1300 Pennsylvania Avenue, N.W.
Suite 350
Washington, D.C. 20004

Mary McDermott
Personal Communications Industry Ass'n
500 Montgomery Street, Suite 700
Alexandria, VA 22314

Michael Altschul
Randall S. Coleman
Cellular Telecommunications Ind. Ass'n
1250 Connecticut Ave., N.W., Suite 200
Washington, D.C. 20036

Douglas N. Letter
Appellate Litigation Counsel
Civil Division
U.S. Department of Justice
601 D Street, N.W., Room 9106
Washington, D.C. 20530

Barry Steinhardt
Shari Steele
Electronic Frontier Foundation
1550 Bryant Street
Suite 725
San Francisco, CA 94103

Kurt A. Wimmer
Alane C. Weixel
Mark E. Porada
Covington & Burling
1201 Pennsylvania Avenue, N.W.
P.O. Box 7566
Washington, D.C. 20044-7566

Martin L. Stern
Michael J. O'Neil
Preston Gates Eillis & Oruvelas Meeds
1735 New York Avenue, N.W., Suite 500
Washington, D.C. 20006

Stewart A. Baker
Thomas M. Barba
Steptoe & Johnson
1330 Connecticut Avenue, N.W.
Washington, D.C. 20036

Eric W. DeSilva
Stephen Rosen
Wiley, Rein & Fielding
1776 K Street, N.W.
Washington, D.C. 20006-2304

Gail L. Polivy
GTE Service Corporation
1850 M Street, N.W., Suite 1200
Washington, D.C. 20036

M. Robert Sutherland
Theodore R. Kingsley
BellSouth Corporation
1155 Peachtree Street, N.E., Suite 1700
Atlanta, GA 30309-3610

J. Lloyd Nault
4300 BellSouth Center
675 West Peachtree Street, N.W.
Atlanta, GA 30375

Joel M. Margolis
Nextel Communications
1505 Farm Credit Drive, Suite 100
McLean, VA 22102

Albert Gidari
Perkins Coie
1201 Third Avenue, 40th floor
Seattle, WA 98101

Pamela J. Riley
David G. Gross
AirTouch Communications
1818 N Street, N.W., Suite 800
Washington, D.C. 20036

Robert M. Lynch
Roger Toppins
SBC Communications
One Bell Plaza, Room 3023
Dallas, TX 75202

John M. Goodman
Bell Atlantic
1300 I Street, N.W.
Washington, D.C. 20005

John T. Scott
Crowell & Moring
1001 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Mark C. Robsenblum
Stephen C. Garavito
AT&T Corp.
Room 3252F3
295 North Maple Avenue
Basking Ridge, N.J. 07920

Douglas I. Brandon
Roseanna DeMaria
AT&T Wireless Services
Fourth Floor
1150 Connecticut Avenue
Washington, D.C. 20036

Kathryn Marie Krause
Edward M. Chavez
U S WEST, Inc.
1020 19th Street, N.W.
Washington, D.C. 20036

William T. Lake
John H. Harwood
Wilmer, Cutler & Pickering
2445 M Street, N.W.
Washington, D.C. 20037-1420

Edward J. Wisniefski
Drug Enforcement Administration
8198 Terminal Road
Lorton, VA 22079

Ronald S. Neubauer
Int'l Ass'n of Chiefs of Police
515 North Washington Street
Alexandria, VA 22314-2357

John Pignataro
New York City Police Department
Building 610, Fort Totten
Bayside, New York 11359

Edward T. Norris
New York City Police Department
1 Police Plaza, Room 910
New York, New York 10038

Carl A. Williams
New Jersey State Police
P.O. Box 7068
West Trenton, N.J. 08628-0068

Harry M. Rivera
Larry S. Solomon
Shook, Hardy & Bacon
1850 K Street, N.W., Suite 900
Washington, D.C. 20006

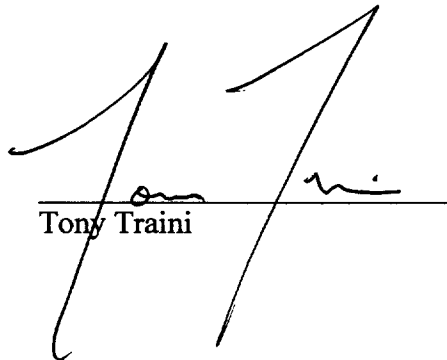
Colette M. Capretz
Fisher Wayland Cooper Leader & Zarago
2001 Pennsylvania Ave., N.W., Suite 400
Washington, D.C. 20006

Carole C. Harris
Christine M. Gill
McDermott, Will & Emery
600 Thirteenth Street, N.W.
Washington, D.C. 20005

Sylvia Lesse
Kraskin, Lesse & Cosson
2120 L Street, N.W., Suite 520
Washington, D.C. 20037

Barbara J. Kern
Ameritech
2000 Ameritech Center Drive
Room 4H74
Hoffman Estates, IL 60196

Lon C. Levin
American Mobile Satellite
10802 Park Ridge Boulevard
Reston, VA 20191



Tony Traini